



6.2.7 Business Continuity Policy

This policy applies to Acknowledge Education and the International College of Hotel Management (ICHM)

1. Purpose

The purpose of this Business Continuity Policy is to ensure that Acknowledge Education (AE) / Stott's College and ICHM (the Colleges) can maintain or rapidly restore critical academic, student support, operational, regulatory, and administrative functions in the event of a significant disruption, crisis, or emergency.

This policy establishes the framework for identifying potential risks, preparing for disruptive events, responding effectively, and recovering operations in a manner that minimises adverse impacts on students, staff, stakeholders, and the Colleges' regulatory obligations and reputation.

This Policy also supports the Colleges' obligations under the Higher Education Standards Framework (Threshold Standards) and the Education Services for Overseas Students (ESOS) legislative framework by ensuring credible business continuity arrangements are maintained to protect educational continuity, student progression, institutional sustainability, regulatory compliance, the Colleges' obligations to overseas students, and the delivery of higher education during significant disruption.

2. Scope

This policy applies to all controlled entities, campuses, organisational units, staff, contractors, consultants, volunteers, students, third-party service providers, and stakeholders engaged by or on behalf of the Colleges.

This policy applies to disruptions including, but not limited to:

- Cyber security incidents and system outages
- Natural disasters and severe weather events
- Pandemics and public health emergencies
- Critical infrastructure or utility failures
- Loss of key personnel
- Third-party supplier disruptions
- Campus access disruptions
- Regulatory or compliance incidents
- Critical incidents affecting student safety or wellbeing

3. Policy Statement

The Colleges are committed to:

- Ensuring the safety, wellbeing, and welfare of staff, students, and stakeholders.
- Protecting critical assets, information, systems, records, and reputation.
- Minimising disruption to students' ability to commence, continue and complete their studies.



- Minimising disruption to teaching, learning, research, student services, and administrative operations.
- Maintaining compliance with applicable legislation, regulatory requirements, and contractual obligations.
- Maintaining credible business continuity arrangements that support the continuity of higher education operations, student progression, tuition assurance obligations, and institutional sustainability.
- Maintaining effective governance, risk management, and crisis management arrangements.
- Ensuring continuity arrangements protect academic quality, academic integrity, student progression, student wellbeing, and continuity of learning and student support services throughout disruption events.
- Implementing business continuity planning processes that are proportionate to operational risk and aligned with sector best practice.
- Regularly testing and reviewing business continuity and emergency response capabilities.

4. Risk Assessment

The Colleges will undertake a Business Impact Analysis (BIA) and business continuity risk assessment at least annually as part of the institutional risk management framework.

The BIA process includes:

- Identification of critical business functions and services.
- Assessment of the impacts of plausible disruption scenarios on critical business functions.
- Identification of dependencies, including personnel, systems, facilities, information, infrastructure, and third-party providers.
- Identification of critical process inputs and outputs.
- Determination of maximum tolerable outage periods and recovery time objectives.
- Assessment of regulatory, academic, operational, financial, reputational, and student impacts.
- Assessment of potential impacts on course accreditation, professional accreditation, student progression, tuition protection obligations, and the Colleges' ability to continue delivering higher education.

The outcomes of the BIA inform recovery strategies and continuity arrangements, including strategies to:

- Protect continuity of critical operational processes and services.
- Maintain the delivery of teaching, learning, assessment, student support and critical academic governance functions.
- Secure alternative arrangements for critical systems, infrastructure, suppliers, or service delivery where feasible.
- Implement alternative operational processes during disruption events.



- Restore normal operations in a controlled and timely manner.
- Maintain data security, privacy, and information integrity during disruption events.

5. Business Continuity Plan (BCP)

The Colleges will maintain a documented Business Continuity Plan (BCP) which outlines:

- Critical business functions and recovery priorities.
- Roles, responsibilities, and delegated authorities during a disruption.
- Incident escalation and decision-making processes.
- Communication protocols for staff, students, regulators, and stakeholders.
- Regulatory notification processes and responsibilities where required under legislation or regulatory requirements.
- Recovery strategies for critical services, systems, and operations.
- Arrangements for alternative teaching, learning, and service delivery where required.
- Contingency arrangements where professional accreditation, course accreditation or registration changes may affect course delivery.
- Cyber incident and information systems recovery arrangements.
- Tuition protection, student transfer and teach-out arrangements where required.
- Training and awareness requirements.
- Processes for post-incident review and continuous improvement.
- The BCP must be accessible to relevant personnel and reviewed regularly to ensure currency and effectiveness.

6. Testing and Review

The BCP will be tested at least annually through exercises, simulations, scenario testing, or other appropriate review activities.

Testing activities may include:

- Desktop exercises
- Loss of course accreditation or adverse regulatory decision scenarios
- Scenario-based simulations
- Evacuation and emergency response exercises
- IT disaster recovery testing
- Communication testing

The CEO, in consultation with the relevant department heads will review the outcomes of testing activities and ensure identified improvements are implemented.

Following any significant disruption or incident, the Colleges will undertake a post-incident review to identify lessons learned and improvement opportunities.



7. Training and Awareness

The Colleges will provide appropriate business continuity training and awareness activities to relevant staff.

Training may include:

- Business continuity responsibilities
- Incident response procedures
- Crisis communication protocols
- Emergency management processes
- Cyber security awareness

The Colleges will also promote awareness of relevant emergency and continuity procedures to students and stakeholders where appropriate.

8. Review

This policy will be reviewed at least every two years, or earlier where:

- Significant operational or regulatory changes occur;
- Material risks or incidents arise;
- Testing identifies deficiencies;
- Or following a significant disruption or emergency event.

9. Responsibilities

Governing Board

- Providing oversight of the Colleges' business continuity and institutional resilience framework.
- Ensuring appropriate governance arrangements are in place to support continuity of critical operations, academic delivery, student wellbeing, and regulatory compliance.
- Monitoring institutional risks that may materially impact the Colleges' ability to operate effectively.
- Receiving assurance from the Chief Executive Officer and Executive Management Team regarding the effectiveness of business continuity arrangements and major incident responses.
- Reviewing significant business continuity incidents, risks, and recovery outcomes where appropriate.
- Satisfying itself that credible business continuity arrangements exist and remain effective through regular assurance reporting.
- Monitoring institutional resilience and the effectiveness of business continuity capability.

CEO

- Ensuring the Colleges maintain an effective institution-wide business continuity management framework.



- Ensuring sufficient resources, systems, and capabilities are available to support business continuity planning and response activities.
- Providing leadership during significant disruptions or crisis events.
- Approving activation of the Business Continuity Plan where required.
- Ensuring appropriate communication with regulators, governing bodies, students, staff, and external stakeholders during major incidents.
- Ensuring appropriate teach-out, tuition protection and student support arrangements are implemented where continuity of course delivery is affected.
- Ensuring continuous improvement activities are implemented following testing exercises or significant disruptions.

Senior Leadership Team

- Providing strategic oversight and support for business continuity planning.
- Ensuring adequate resources are allocated to business continuity management.
- Approving, maintaining, and reviewing the Business Continuity Plan (BCP).
- Ensuring appropriate testing, training, and awareness activities are undertaken.
- Overseeing institutional responses to significant disruptions and critical incidents.
- Ensuring appropriate escalation, reporting, and regulatory notification obligations are met where required.

Organisational Unit Heads

- Ensuring their operational areas maintain continuity procedures aligned with the BCP.
- Identifying and reporting operational risks and vulnerabilities.
- Maintaining local continuity arrangements for critical functions.
- Participating in continuity testing and incident response activities.
- Communicating relevant continuity procedures to staff and stakeholders.

Staff

All staff are responsible for:

- Complying with this policy and associated procedures.
- Participating in required training and awareness activities.
- Reporting incidents, disruptions, or risks that may impact continuity of operations.

10. Related Documents

6.2.6 Business Continuity Plan

6.2.3 Critical Incident Policy and Procedure

6.2.2 Health and Safety Policy

6.2.10 Risk Management Policy

Emergency Management Plan (EMP)_ Stott's College

6.2.4a Risk Appetite Statement AE

6.2.4b Risk Appetite Statement ICHM

6.1.1a Acknowledge Education Governance Framework



6.1.1b ICHM Governance Framework
6.2.1 Delegations Framework
5.3 Quality Assurance Framework
HE Risk Register_AE and ICHM
VET Risk Register_AE
Child Safety Risk Register_Stotts College (Acknowledge Education)

11. Policy Information

Policy Name	Business Continuity Policy
Document Number	6.2.7
Purpose	Ensuring that the Colleges can maintain or rapidly restore critical academic, student support, operational, regulatory, and administrative functions in the event of a significant disruption, crisis, or emergency
Audience	☒ Staff ☐ Students ☐ Public
Category	Governance and Accountability
Subcategory	Corporate Monitoring and Accountability
Approval Date	25/10/2023
Effective Date	25/10/2023
Date of Last Approval	24/09/2026
Review Date	24/09/2028 (2 year review cycle unless required earlier per section 8 of this policy)
Responsible Officer	CEO
Approving Authority	Board of Directors
Contact	Regulatorcompliance@ae.edu.au

12. Change Log

Date	Version	By	Notes
01/09/2023	1.0	Thiago Candeu (Head of Ops)	Creation
14/05/2026	2.0	HQR	Review and update, restructure and coverage of AE and ICHM, strengthening of policy terminology, change responsible officer from Head of Operations to CEO, expanded responsibilities section, reviewed and strengthened alignment with HESF Amendments.